Towards the Digitally Named World : Challenges for New Social Infrastructures based on Information Technologies

安浦, 寛人
システムLSI研究センター　九州大学

出版情報：Proceedings of Euromicro Symposium on Digital System Design -Architectures, Methods and Tools-(DSD2003), pp.17-22, 2003-09
バージョン：
権利関係：

Towards the Digitally Named World
-Challenges for New Social Infrastructures based on Information Technologies-

Hiroto Yasuura
System LSI Research Center
Kyushu University, Fukuoka, Japan
yasuura@slrc.kyushu-u.ac.jp

Abstract

In the 21st century, social infrastructures, such as economic systems, transportation systems and governmental service systems, are redesigned and reconstructed based on information technologies. In this paper, basic information technologies of the new social infrastructures are proposed. The Personal Identifier (PID) system for bidirectional authentication and an RFID tag system will play important roles in the new social infrastructures. Using PID and RFID tag, we can bridge a gap between the real world and the virtual world on computers automatically. We call the society, in which all persons and goods have their own digital names and recognizable both in the real and virtual world, "Digitally Named World". The systems require technologies of SoC, networking, security and software. Technical challenges and social requirements for the new technologies are presented.

1. Introduction

In the last three decades of the 20th century, many information and communication technologies have been developed and also introduced in social infrastructures, which are supporting our daily lives. Government services, economical activities, energy supply, transportation services and communication services are provided based on the social infrastructures. Since the information technologies progresses very rapidly, the basic structure of each social infrastructure, which was mostly designed in the 19th or the beginning of 20th centuries with few possibility of information technology, cannot follow the new technological progress and should be redesigned with an assumption of the existence of the advanced information technology.

One of the largest challenges of this century is to establish and reconstruct the social infrastructures using the advanced information technology. Based on the high-performance SoCs (System on a Chip) connected by wide-band world-wide networks, we can design basic concepts of the next generation of each social systems. It includes an electrical voting system, which will change the implementation of democracy and governmental systems. Electrical commerce systems and electric money leads drastic changes of the global economic system. They are directly related with the tax collection, the individual property and the national finance. They also related with the basis of the fundamental social structure including individual rights and national security.

We need discussions on not only the technically possible solutions and their implementation techniques but also the direction of technical developments like how we keep the stability of the society and how we implement the safe and comfortable society. The final question is "what kind of society should we build up?" It is not a pure technical question but we have to start open discussions with various people including social scientists, statesmen, economists and all of citizens.

In this paper, we introduce two social infrastructure information technologies. The Personal Identifier (PID) system is an infrastructure for bidirectional mutual authentication, which will be used for electric commerce and governmental services [1]. An RFID tag system is also important technology to implement efficient management of products and economic activities. Using PID and RFID tags, we can bridge a gap between the real world and the virtual world on computers

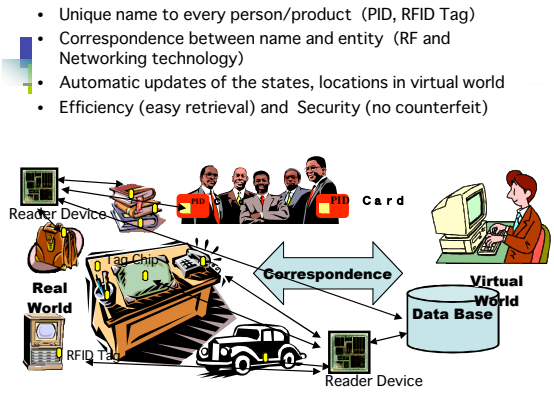

Fig. 1 Digitally Named World

automatically [2] [3]. We call the society, in which all persons and goods have their own digital names (identifiers) and recognizable both in the real and virtual world, "Digitally Named World" (See Fig. 1). The systems require technologies of SoC, networking, security and software. Here, technical challenges and social requirements for the new technologies are presented. Some people are afraid of the infringement of their privacy in the digitally named world. Our discussions also include the technology to protect privacy and individual rights as well as efficiency and stability of the society.

2. Requirements for Social System Infrastructure

For the redesign of social infrastructure in the 21st century, there are several points that we have to discuss and consider.

1) Protection of the individual right;

The social system should be designed for protecting individual rights as well as maintaining public order. Protection of organizations and systems from various possible attacks and disasters has been mainly considered in social system design such as banking systems and governmental systems. Since the next generation of social systems are inherently and closely involved in a daily life of citizens, protection of individual privacy and rights should be the primary concern of social system designers.

2) Simple mechanism;

The basic structure and concept of the system should be simple. It is important that system users can intuitively understand basic mechanism of the system and naturally understand the risks and user's responsibilities in their usage. A black box that users can hardly see the essential part of the system is very dangerous.

3) Reliability and Stability;

Social infrastructure should have high reliability and be stably available for more than ten years. The reliability and stability of the system are directly affects safety of human life, property and privacy strongly relying on the system.

4) Flexibility and Extensibility;

The system should be flexibly designed to employ the most advanced technologies, which are rapidly progressed. Grand design of social infrastructures is required for avoiding fundamental structure changes of social systems in spite of any technological changes.

5) Security and Easy-Recoverability;

The system should be secure against intentional attacks and accidents. The system should also be easily recovered, if it fails by attacks or accidents. Minimization of the damage and the cost of recovery is an important factor of the system design.

6) Economical Feasibility;

The system should be economically built and operated as a social infrastructure. The cost of operation and maintenance is important as well as the cost of devices and system integration. Since the number of devices used in the system is very large,

total energy consumption is also important criteria of design.

3. User Authentication based on PID [1]

In the realization of e-commerce and e-government, mutual authentication between partners communicating each other through a network is fundamental technology. The authentication system must be bidirectional and have a mechanism that takes the protection of individual privacy into consideration. The system should be easy to understand its fundamental concept and structure. It should have high reliability and ability to recover from damages by attacks and accidents. It is also important that the system reflects the trust and credit relationships among individuals and organizations.

The present password used ATM is a method to protect an organizations and a system in a unilateral way. Therefore it is hardly to say "mutual authentication." Using the biometrics like fingerprint is still not "mutual" and has a fatal fault. If information on a fingerprint is leaked, it cannot be changed again. Although the new approaches like PKI and One-Time-Password based on public key encryption have been proposed, many of them have complicated mechanisms which are difficult to understand intuitively by ordinary users.

The PID system, which is proposed here, has an extremely simple mechanism and is based on the existing social trust relationship. Individual authentication using PID consists of three kinds of participants– PID Issuers, Users, and Service providers. Issuers are various kinds of organizations that individuals belong to (Communities, Companies, Schools, Credit card service companies, etc). Issuers are basically assumed to have a duty to protect their individual participants. This social trust relationship is the basis for the PID system.

Assume a person A is a member of an organization B, which is the PID issuer in this context. The issuer B examines A's personal identity, and decides if A is deserved to be authenticated or not. When B determines to give the authentication to A with B's responsibility, the issuer B gives A "a Personal Identifier", called PID, that is a long bit sequence (ex. one million bits). This sequence is stored in storage media like an IC card and the card is issued to A.(See Fig.2)

When a service provider C, who deal with services to users, want to make an e-commerce service to the members of the organization B, the provider C applies to the issuer B for permission of usage of the PID system issued by B. The issuer B investigates confidence of the provider C whether the services provided by C are beneficial and harmless for the members of B. When B determines that it is beneficial for the members, B provides a part of PID of each member (ex. 100 bits, we call it a sub-PID) to the service provider C. B also notifies the members that the sub-PID of each PID have been given to C. The person A is now a user of the services provided by C. The user A and service provider C mutually authenticate using this sub-PID each other. A method of mutual authentication using the sub-PID is not prescribed in the PID systems. A and C can adopt a method of authentication from various ways such as One-Time-Password and common key encryptions.

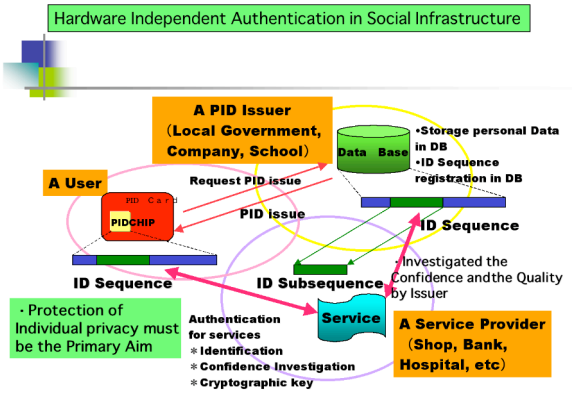

Fig.2 The PID System

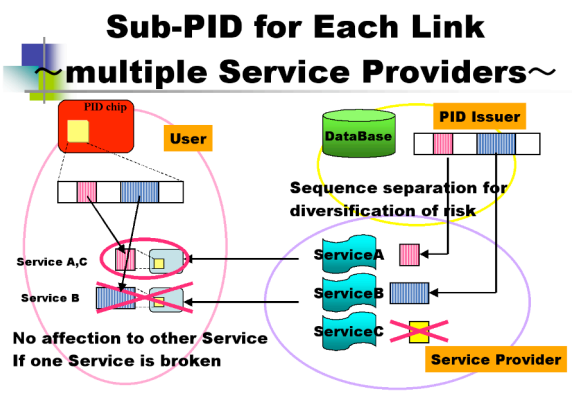

Fig.3 Usage of Sub-PID for Each Service

The PID system provides a fundamental mechanism for mutual authentication based on social trust relationship independent of each service. The advantages of the PID systems are concluded as follows.

1) It is the most primitive mutual authentication. Distinct secret information, a sub-PID, is assigned to each link of communication between a user and a service provider. If the sub-PID is leaked, the damages are limited only the corresponding link between them. All other links connecting different services to the user and other users to the service are safe.(See Fig.3)
2) Users can understand the concept of the mutual authentication easily and intuitively without knowledge of complicated algorithms of authentication methods.
3) A user need not tell his/her private information such as his/her name and address to service providers for getting services. It leads to protection of privacy from data mining. In the PID systems, the issuer guarantees creditworthiness of each user as well as creditworthiness of service providers.
4) Considering trading off of energy consumption, costs and security levels, mutual authentication methods can be chosen independently of the PID system. Since the PID system is designed independently of the methods of mutual authentication and other implementation factors, it universally and stably works under the expected technology advancement.
5) Service providers only have to care of the sub-PID of each user and do not receive privacy information of individuals. The cost to maintaining the security can be drastically cut down, because the damages and responsibilities of providers are minimized. Even if sub-PID's provided to a service provider are leaked, the issuer cancels the old sub-PIDs and assign other part of PID as new sub-PIDs. The recovery cost will be a small amount.
6) A User can obtain several PIDs which are issued by different organizations that he/she socially belongs to. The user can use a combination of the PIDs to control the security of communication and distribute various kinds of potential risks. (See Fig.4)

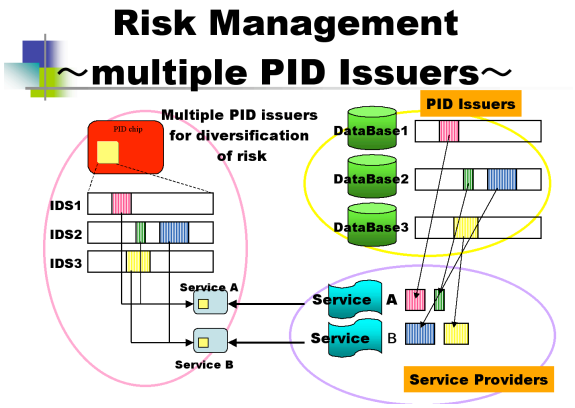

Fig. 4 Combination of PIDs Issued by Different Issuers

These are many technological problems to be solved, when the PID system is realized.

1) Mutual authentication method;

Various methods for mutual authentication using sub-PID should be developed. Service will chose one of the methods satisfying constraints of cost, energy consumption, usability and security.

2) Devices to store PID;

The integration of security and portable technologies such as tamper resistance, low power technology, radio-frequency communication and cryptography is needed.

3) PID management techniques;

PID management techniques for issuers, users, and the service providers are requested. Security and reliability of the total system is important. Not only technical problems but also social problems should be discussed carefully before introduction to the real world.

4) Constructing techniques for application systems;

We need to develop a security policy of each application system to use PID and basic technologies for its realization. Minimizing energy consumption all over the system is also important.

3. RFID Tags and its application [2] [3]

While the PID system is a basic system for digital naming for individuals, the foundation of digital naming for goods and products is RFID (Radio-Frequency Identifier) tags. The recent years, many systems used RFID tags are proposed and implemented.

RFID tags are attached to many kinds of products, and they are used to recognize and identify them. The bottleneck of the present information processing is that various events occurred in the real world are not smoothly reflected in the virtual world on a computer system. For example, when we register furniture on Data Base system, it is easy to manage on the computer. But it is not so easy to reflect transitions of the furniture and change of conditions and status of them in the real world automatically. Actually, big amount of labor and costs are spent for checking up the location of furniture and updating the Data Base. RFID tag is a solution to reduce the time consuming task. For example, book management at libraries has required large man power, but an RFID tag system is now connecting books on shelves to corresponding data on a library data base automatically.

In usage of the RFID tags in the products management, it is important to reuse effectively the same tag in the different stages during a lifecycle of products. Each stage of the lifecycle of products consists of the following managements:

1) supply parts, production and quality managements in the production stage
2) distribution and sales managements, and ensure of traceability in the distribution stage
3) ownership, antitheft, and maintenance service managements in the user service stage
4) material sorting in the recycle stage.

(See Fig.5.)

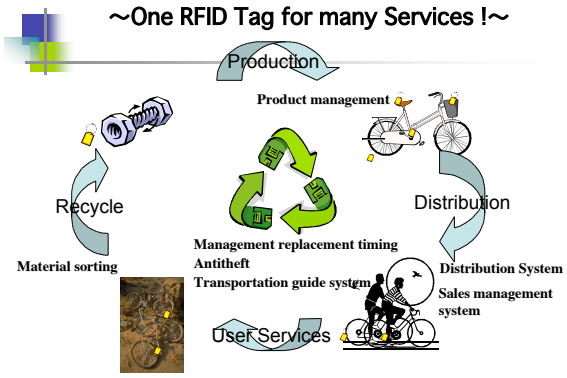

Fig.5 Product Lifecycle

To reduce the cost of RFID tag system, it is important to commonly use one RFID tags at each stage of the products lifecycle. However, once a unique ID number is given to a product, there is a problem that behavior of holder's can be traced through the ID number and privacy information is indirectly leaked without holder's knowledge.

To resolve these privacy problems, we proposed a system that switches the public ID to private ID. Public ID is standardized by ID allocation method decided by standard organization and IDs are assigned to all products. Public IDs are memorized in ROM and used in the production, distribute and recycle stages. On the other hand, there is a request for public ID to be unreadable from the outside to protect individual privacy in the user service stage. Therefore a user can overwrite the private ID when the ownership is given to him/her. Private IDs are stored in a rewriteable nonvolatile memory (RAM) and as long as this is available, During the RAM mode, public ID cannot be read from outside. Switching two kinds of ID numbers, the leakage of

privacy information can be controlled. When you discard it, private ID is eliminated and public ID is used again in recycle stage. (See Fig.6.)

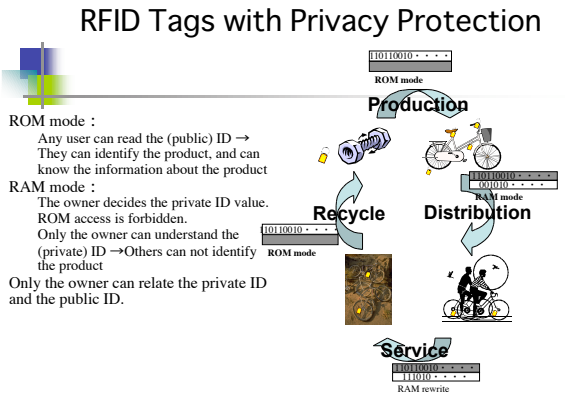

Fig. 6 Privacy Protection Mechanism

Various applications are considered in production and distribution stages. In the user service stage, services combining with the PID system are considered for various applications. Users can manage their properties without leaking the privacy information. Of course, to rewriting of private ID, a means of encryption is needed. To build efficiently a well-organized social infrastructure using RFID tag chips, we have to resolve the following problems:

1) Tag chips that can be easily attached to various products with low cost (less than 1cent),
2) A system architecture for protecting privacy,
3) A wide area tracking system combining distributed Data Base and network technologies,
4) Low cost reader and backend network devices.

5. Conclusion

Designing a new social infrastructure based on advanced information technology is a great challenge and it is also design of the future of our society. The PID system and the RFID tag system will be basic infrastructures to implement a stable, safe and efficient society. Individual rights and privacy must be protected by information technology.

We are designing an experimental system of Digitally Named World with PID and RFID tags in our new campus, which is to be opened in 2005. Various services for students, workers and professors are scheduled. The new campus will be a model of the future society with the advanced social information infrastructure.

Acknowledgement

We thank Dr. S. Inoue, Mr. Y. Hamasaki and Mr. S. Noutomi for their help of preparation of this article. Thanks are also due to all of members System LSI Research Center of Kyushu University. This work has been supported in part by the Grant-in-Aid for Creative Scientific Research No.14GS0218 of the Ministry of Education, Science, Sports and Culture(MEXT) from 2002 to 2006 and Silicon Sea-Belt Project "Establishing Project of a Cluster for System-LSI Design and Development".

References

[1] Y. Hamasaki and H. Yasuura, “A Propsal of Secure Information Infrastructure Based on PID” In the Proceedings of DICOMO2002, July., 2002. and also published in Research Reports on Information Science and Electrical Engineering of Kyushu University, Vol.7, No. 2 pp.139-148, Sept., 2002. (in Japanese)

[2] S. Inoue and H. Yasuura, “Towers the Digitally Named World with Security and Convenience Using RFIDTags”, Research Reports on Information Science and Electrical Engineering of Kyushu University, Vol.7, No. 2 pp.131-138, Sept., 2002. (in Japanese)

[3] S. Inoue, S. Konomi, and H. Yasuura, “Privacy in the Digitally Named World with RFID Tags”, Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing, Sept., 2002.